

(12) UK Patent Application (19) GB (11) 2 168 573 A

(43) Application published 18 Jun 1986

(21) Application No 8431421

(22) Date of filing 13 Dec 1984

(51) INT CL⁴
H04L 9/00

(71) Applicant
STC plc (United Kingdom),
190 Strand, London WC2R 1DU

(52) Domestic classification (Edition H):
H4P DCSS

(72) Inventors
William Arthur George Walsh
Dennis Gordon Froggatt

(56) Documents cited
None

(74) Agent and/or Address for Service
S R Capsey,
STC Patents, Edinburgh Way, Harlow, Essex CM20 2SH

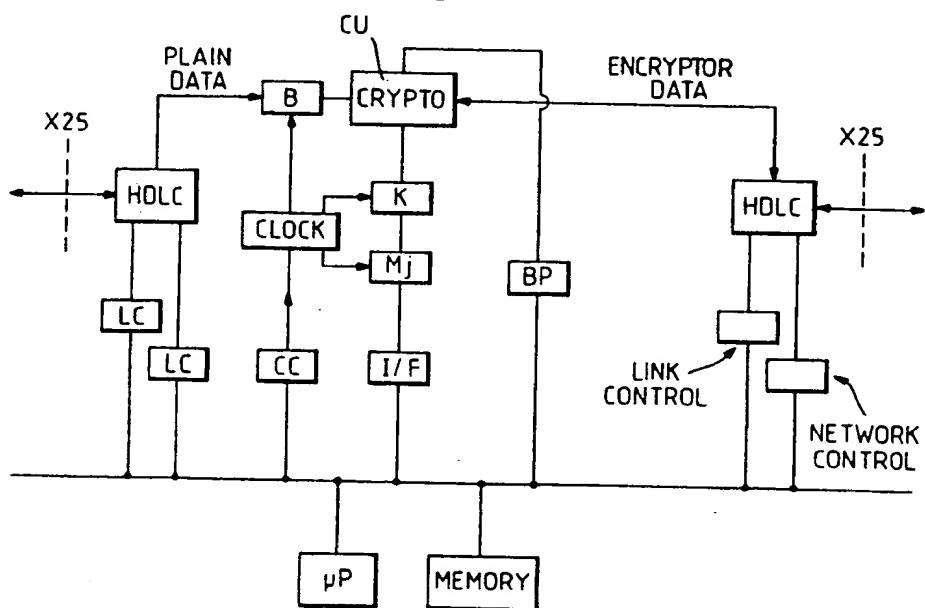
(58) Field of search
H4P

(54) Packet switched system

(57) End-to-end encryption of traffic in packet networks presents difficulties due to the discontinuous nature of the data. In the present method these difficulties are overcome by sending an initialisation variable (IV) during the initial call setting and controlling the clocking information such that at each end the clock for the encryption or decryption is started at the beginning of the information field and stopped at the end thereof. Thus when the next packet is sent, both cryptos are correctly set.

This avoids the need to send such information with each packet, as called for in some known systems.

Fig. 1.



GB 2 168 573 A

1/2

2168573

Fig. 1.

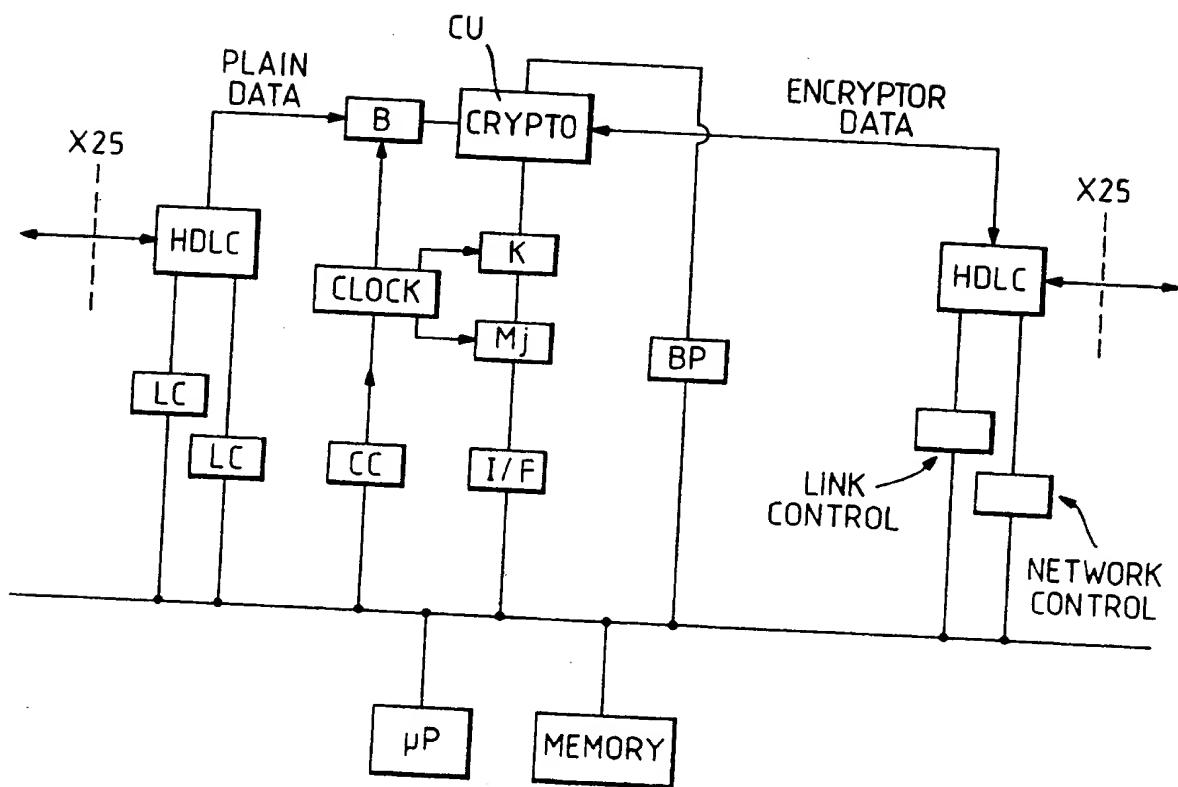
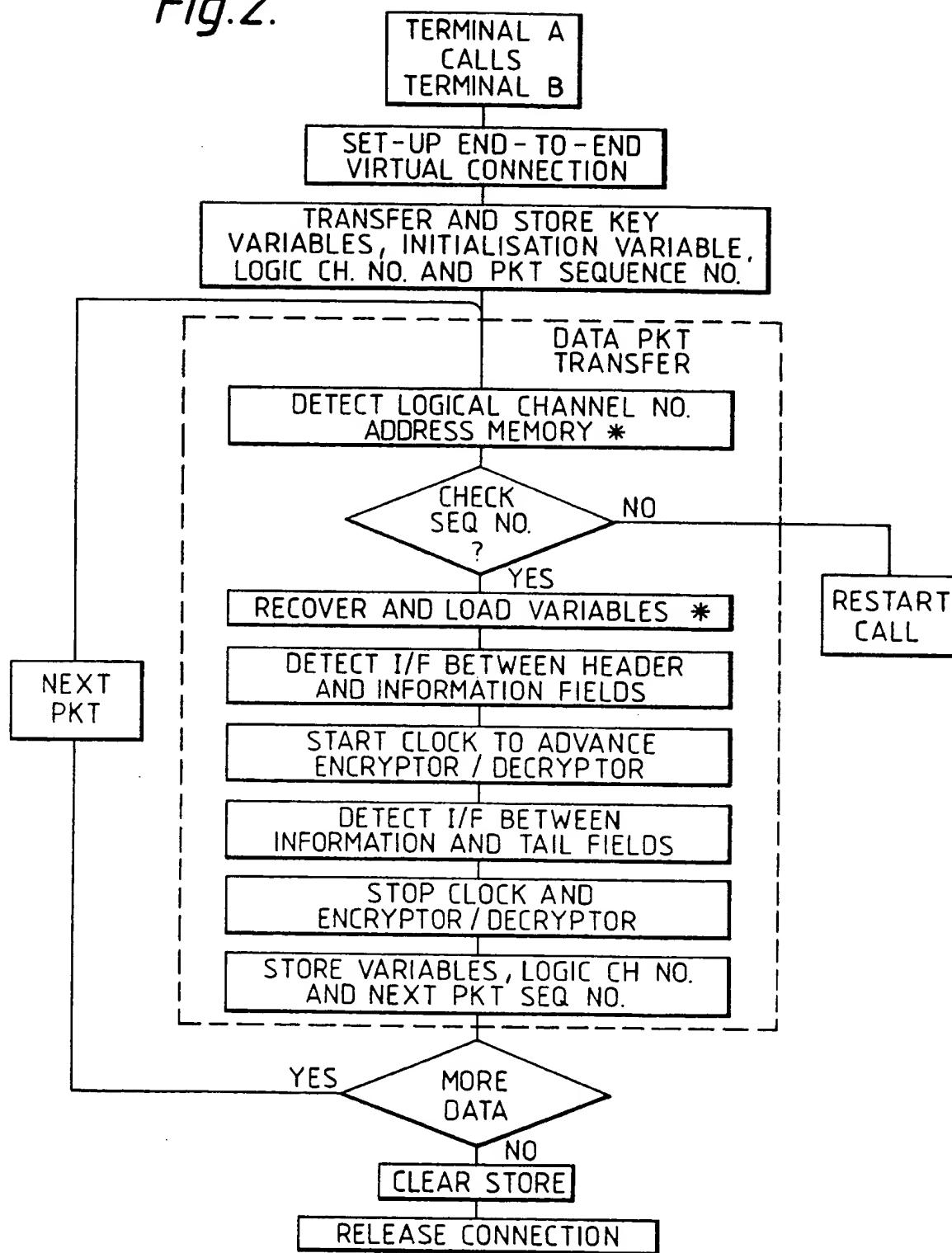


Fig.2.



SPECIFICATION

Packet switched system

- 5 This invention relates to data transmission systems in which data is conveyed in packet-switched manner. In such systems the packets which together form a message may well have to be sent from a calling terminal to a called terminal via two or more exchanges or nodes.

10 Security is essential in some cases of communication of information through networks, particularly for data relating to financial transactions, electronic mail etc. Security involves such aspects as authentication of access to information, authentication of data sent by signatures, and protection of traffic from deliberate interference or intervention while in transit 15 through the network which may be public or private, circuit or packet switched, telephony, data or both.

20 The arrangement to be described herein relates to the end-to-end encryption of traffic in packet networks in which the prior art has 25 limitations in application and effectiveness.

25 Information is transmitted in packet networks by arranging the data in a framed format such that data link control and error detection information is in the frame. Frames 30 may be concatenated to form a contiguous data stream or, more likely, sent in groups each frame being separated by a variable length delay. In interactive operation the information content of packets may be small and 35 the separation may be relatively long. To operate the network efficiently, packets for other transmissions are interposed in the intervening spaces.

40 End-to-end encryption must ensure that only the information content of the packet is encrypted since the control information in the frame is needed at intermediate nodes in the network. To decrypt the information, certain 45 encryption parameters must be transmitted to the receiving end to load the decryption devices, and data-related synchronism must be maintained although the data is separated by different time intervals at transmitter and receiver.

50 Prior art exists in which an Initialisation Variable, IV is sent with each packet and is used at the receiver to reset the decryption device and thus maintain synchronisation. However, 55 this has limitations including:

(a) The standard frame format e.g. X25, requires modification to accommodate the additional IV.

60 (b) The IV which may be 64 bits long is a significant increase to the framing "overhead". (c) When contiguous packets are sent the increased overhead may involve an increase in the required transmission rate which may exceed the constraints of the system.

65 A variation exists in which the IV is sent

with an initial packet and with succeeding packets if, and only if, the duration between packets exceeds the duration of the IV. This method can only be applied to link encryption 70 (Level 2) since the variable delay and multiplexing encountered in a node disturbs the synchronisation between packets.

An object of the invention is to provide an improvement on the known arrangements referred to above.

According to the invention there is provided a data transmission system of the packet switched type, in which each message to be transmitted consists of one or more data 80 packets each having a header, an information field which may be encrypted, and a tail, in which an initialisation variable is transmitted from the one end of the connection to the other end thereof only during the initial call 85 setting signalling and is used to set the encryption and decryption operations to the same state, in which at the sending end, the end of the header is detected and controls the commencement of the encryption operation 90 during the information field and the start of the tail is detected to stop the encryption operation, and in which at the receiving end, the end of the header is detected and controls the commencement of the decryption operation 95 and the start of the tail is detected to stop the decryption operation, so that between packets the encryption and decryption operations are stopped in exactly similar states.

100 Embodiments of the invention will now be described with reference to the accompanying drawings, in which Fig. 1 is a simplified schematic of part of a terminal embodying the invention, while Fig. 2 is an explanatory flow diagram.

105 The present method enables the packetised traffic to be so encrypted that the control overhead associated with each frame is not extended but nevertheless synchronism between encryption and decryption processes is achieved at all times. Thus the information throughput of a transmission, store and forward, system can be maintained without modification to normal operation.

110 The present method is based on the premise that packet traffic is asynchronous (although a bit synchronous bearer may be used), and that packets can be of variable length and variably spaced. During the establishment of a connection—virtual or real 115 agreement is reached on the need to apply encryption, the necessary key parameters being exchanged. The initialisation variable is sent with this initial exchange and is used to reset both encryption and decryption devices 120 to the same initial condition.

125 A bit rate clock is generated such that bit synchronism is assured at each end, and that the commencement of the encrypted data content of the packet causes the crypto devices to be advanced from their initial condi-

tion. At the end of the encrypted data, the clocks are interrupted, thus stopping both crypto devices at the same position. The successive packets cause the cryptos to restart 5 and stop respectively at the beginning and end of each encrypted sequence of data. Thus since the cryptos always restart from the same position in which they were stopped, synchronism between the encryption and de-10 cryption devices is generally maintained.

If an external agency disturbs this synchronism, the loss is detected by normal error detection methods used in the system, and an error message is returned to the sending end 15 to request a new initialisation variable, and repeat of the data.

A variation of the present method involves the use of so called 'fast select' procedures in which the whole of the information is in a 20 single packet together with the required address and control information. In this case, the type of packet is identified by a 'facility' code and the encryption and initialisation parameters are within fields preceding the information 25 field. Thus the decryption device is aware of the special type of packet and having been appropriately set starts the algorithm process at the beginning of the information field.

The present system is described as applied 30 to a system of the internationally standardised X25 type, which allows for multiple logical channels to be associated with a single physical link. This complicates the operation of the encryption unit in that between packets it 35 needs to store the logical channel number in association with the appropriate state of the initialisation variable. Therefore, as each logical channel is transmitted over the physical link it is compared with those in store and the re-40 quired IV transferred into the working IV memory.

Fig. 1 shows as much of an X25 based 45 encryption/decryption unit as is relevant to the present method, the remainder of such a terminal following conventional practice. Information arriving at the unit possibly for encryption enters at an HDLC (high level data link control) unit, which among other functions extracts 50 any control information for the link control LC and network control NC blocks. The information passes from the HDLC block to a buffer B for temporary storage. From here it passes, under clock control, to a crypto unit CU from 55 which the packets, with their information fields encrypted if needed, pass to another HDLC unit for transmission.

Associated with the crypto unit CU, there 60 are a key unit K from which the crypto key is obtained, both when the unit CU is encrypting and also when it is decrypting. Also we have the initialisation variable (IV) generation unit IVU; when a call is set up under control of the microprocessor MP, the call setting information which is initially sent includes encryption 65 keys and an initialisation variable. This

notifies the called end as to whether or not the message to be sent is encrypted, this being determined from part of the message as it arrives via the first HDLC block.

70 The clock is so set, under microprocessor control, that when the first packet is sent, the crypto unit CU is enabled at the commencement of its information field, and is stopped at the end of that field.

75 At the called end, which is similar to what is shown, the initialisation variable is passed via the link control LC thereat to the microprocessor and clock thereat, so that the microprocessor sets the called end's crypto for the desired encryption. In addition, when the first packet arrives, the clock is enabled so as to start the crypto unit at the commencement of the information field and to stop at the end thereof. The initial call setting operations will, 80 of course, in accordance with normal practice, have resulted in the clocks at the two ends having been brought into synchronism.

Thus when the information field of the first packet ends, we have both crypto units

90 clocks stopped at the same point. When the next packet is sent, both clocks are started at the start of the information field, and they both start from the same point in time. Thus encryption and decryption take place, with the 95 clocks, and thus the crypto devices starting from the same point. When the information field ends, both clocks again stop. Hence the system only needs one initialisation variable per multipacket message.

100 To express the system in a slightly different manner, we have the following summary, which should be studied in conjunction with the flow diagram, Fig. 2. note in Fig. 2 that the two blocks marked with asterisks are not required in a single channel system.

(a) What is Required

110 A packet communication system using packets with defined headers and tails, which system has encryption and decryption at each end, and has clock control at each end.

(b) How the System Operates

- 115 (1) Set up end-to-end connection.
- (2) Transfer IV (keys may also be transferred).
- (3) Encryptor and decryptor static and may be headed with IV.
- (4) Send packet.

120 AT EACH END:

- (5) Detect end of header.
 - (6) Start clock and encryptor/decryptor at commencement of information field.
 - (7) Detect start of tail.
 - 125 (8) Stop clock and encryptor/decryptor at end of information field.
- THEN
- (9) Encryptor/decryptor static and loaded with some variables.

(10) Repeat (5) to (8) for next packet.

Thus the above method permits encryption to be applied to the communication of data through a packet network without the need to significantly alter the traffic flow. It has the following advantages:

(a) Encryption key and initialisation parameters can be incorporated into call set-up procedures.

10 (b) Encryption parameters are not required to be sent with each packet when a call consists of many packets.

(c) The encrypted packet may be

15 transmitted at the same rate and for the same duration as the corresponding unencrypted packet.

(d) It is not required to amend existing Level 2 (HDLC) frame formats and amendments to higher level procedures are easily accommodated.

(e) The method is particularly applicable to packetised voice communication where real time integrity is of importance and packets are kept short.

25 (f) The method can be applied to data already formatted into standard packets e.g. X25.

(g) The method is compatible with the requirements of 'fast select' operation.

CLAIMS

1. A data transmission system of the packet switched type, in which each message to be transmitted consists of one or more

35 data packets each having a header, an information field which may be encrypted, and a tail, in which an initialisation variable is transmitted from the one end of the connection to the other end thereof only during the

40 initial call setting signalling and is used to set the encryption and decryption operations to the same state, in which at the sending end, the end of the header is detected and controls the commencement of the encryption operation

45 during the information field and the start of the tail is detected to stop the encryption operation, and in which at the receiving end, the end of the header is detected and controls the commencement of the decryption operation

50 and the start of the tail is detected to stop the decryption operation, so that between packets the encryption and decryption operations are stopped in exactly similar states.

55 2. A system according to claim 1, in which the encryption and decryption operations are controlled by starting and stopping their appropriate clocks.

60 3. A system according to claim 1 or 2, in which call setting signalling, initialisation variable and encrypted information are all contained within a single packet.

65 4. A system according to claim 1, 2 or 3, in which packets belonging to different virtual connections are multiplexed, in which at the

end of a packet in the static state the cryptographic variables are transferred to a memory and during the header of the next packet the relevant cryptographic variables are loaded from memory.

5. A data transmission system of the packet switched type, in which each message to be transmitted consists of one or more data packets each having at least a header, an

75 information field and a tail, in which when a message to be conveyed is to be encrypted an initialisation variable is transmitted from the calling end of the connection to the called end thereof during the initial call setting signalling,

80 in which at the sending end the encryption operations start at the beginning of the information field and end at the termination of the information field, in which at the called end the receipt of the initialisation variable sets the

85 decryption means to its initial state appropriate to the decryption of the packets to be received, in which at the calling end the termination of the information field of a packet leaves the clocking means at the calling end in

90 a state appropriate to the commencement of encryption of the information field of the next packet, and in which at the called end the termination of the information field of a packet being received and decrypted leaves the

95 clocking means in a state appropriate to the start of the information field of the next packet, whereby the initialisation variable is only sent once for a multipacket message, and is sent separate from the message packets.

100 6. A data transmission system of the packet-switched type substantially as described with reference to the accompanying drawings.

Printed in the United Kingdom for
Her Majesty's Stationery Office, Dd 8818935, 1986, 4235.
Published at The Patent Office, 25 Southampton Buildings,
London, WC2A 1AY, from which copies may be obtained.